CLAIMS

1. A method for establishing a communication session on a communication medium between a first data processing station and a second data processing station having access to the communication medium, comprising:

receiving at the first station a request from the second station for initiation of a communication session;

producing dynamic sets of session random symmetric encryption keys at the first station; and

after receiving said request, executing a plurality of exchanges of encrypted messages across said communication medium to mutually authenticate the first station and the second station, and to provide the encryption key to the second station for use in said communication session.

2. The method of claim 1, wherein during said plurality of exchanges, said first and second stations use at least two shared secrets, which are shared between the first station and the second station, or between the first station and a user at the second station, without exchanging messages carrying said shared secrets via the communication medium.

3. The method of claim 1, including mutual authentication based on at least two shared secrets, without exchanging messages carrying said shared secrets in any form via the communication medium.

4. The method of claim 1, wherein said plurality of exchanges comprise interactive exchanges, said interactive exchanges including a message from the first station to the second station and a responsive message from the second station to the first station, where the responsive message comprises information from the message from the first station derived using information derived from a message in a previous exchange.

5. The method of claim 1, wherein producing an encryption key at the first station includes:

assigning a session random key in said first station, in response to a request received by said first station during a session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and

wherein said plurality of exchanges includes at least one message carrying an encrypted version of one of said plurality of intermediate data random keys to be accepted as said encryption key upon said mutual authentication.

6. The method of claim 1, wherein producing an encryption key at the first station includes:

providing a buffer at the first station;

generating keys and storing said keys in the buffer;

associating respective session random key initiation intervals with said keys stored in said buffer;

using keys from said buffer as session random keys in response to requests received by said first station during said respective session random key initiation intervals for use in a first exchange of said plurality of exchanges;

removing keys from said buffer after expiry of the respective session random key lifetime in the buffer.

7. The method of claim 6, wherein said buffer is managed as a circular buffer.

8. The method of claim 6, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a multiple M times said value of session random key lifetime to engage into establishing a communication session, where M is less than or equal to 10.

9. The method of claim 6, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a multiple M times said value, and the session random key lifetime to engage into establishing a communication session is less than about 90 second

10. The method of claim 1, wherein producing an encryption key at the first station includes:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;

wherein said plurality of exchanges includes a first message from the first station carrying said session random key to the second station, where the second station returns a second message carrying a shared parameter, which is shared between the first station and the second station, or between the first station and a user at the second station, and encrypted using the session random key; and

decrypting the shared parameter from said second message at the first station.

11. The method of claim 1, wherein producing an encryption key at the first station includes:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;

wherein said plurality of exchanges includes

a first exchange including sending a first message from the first station carrying

said session random key to the second station, where the second station returns a second message carrying a shared parameter encrypted using the session random key, and decrypting the shared parameter at the first station to validate the second station, or a user at the second station; and

a second exchange including sending a further message from the first station to the second station, the further message carrying a particular data random key from said plurality of intermediate data random keys encrypted using the session random key, where the second station returns another message carrying a hashed version of said particular data random key encrypted using said particular encryption key to the first station, and decrypting said hashed version of said particular data random key at the first station using said particular data random key.

12. The method of claim 1, wherein producing an encryption key at the first station includes:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and

after said request for initiation of a communication session, presenting to the second station a user interface along with the session random key, said user interface including a prompt for entry of a shared parameter and at least one shared secret.

13. The method of claim 1, wherein producing an encryption key at the first station includes:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and

after said request for initiation of a communication session, presenting to the second station a user interface along with the session random key, said user interface including a prompt for entry of a shared parameter and at least two shared secrets.

14. The method of claim 1, wherein producing an encryption key at the first station includes:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;

wherein said plurality of exchanges includes

a first exchange including sending a first message from the first station carrying said session random key to the second station, where the second station returns a second message carrying a shared parameter encrypted using the session random key, and decrypting the shared parameter at the first station; and

a second exchange including sending a third message from the first station to the second station, the third message carrying a particular data random key from said plurality of intermediate data random keys encrypted using the session random key, where the second station returns a fourth message carrying a hashed version of said particular data random key encrypted using said particular data random key to the first station, and decrypting said hashed version of said particular data random key at the first station using said particular data random key;

and then executing at least one additional exchange in said plurality of exchanges, where

said at least one additional exchange includes sending an additional message from the first station to the second station carrying a next data random key from the plurality of intermediate data random keys associated with said request, encrypted using a key exchanged during a previously completed exchange in said plurality of exchanges, where the second station decrypts said next data random key and returns a responsive message carrying a hashed version of said next data random key encrypted using said next data random key, and decrypting at the first station said hashed version of said next data random key using said next data random key.

15. The method of claim 14, including during at least one of said additional exchanges,

producing said third message by first veiling the particular data random key using a first conversion array seeded by a first shared secret and encrypting the veiled particular data random key, where the second station decrypts and unveils said particular data random key using the first shared secret, and where the second station produces said fourth message by veiling the hashed version of the particular data random key using a second conversion array seeded by said first shared secret and encrypting the veiled hashed version of the next data random key; and

decrypting and unveiling the hashed version of the particular data random key at the first station.

16. The method of claim 14, including executing more than one of said additional exchanges.

17. The method of claim 14, including during at least one of said additional exchanges,

producing said additional message by first veiling the next data random key using a first conversion array seeded by a shared secret and encrypting the veiled next data random key, where the second station decrypts and unveils said next data random key using the shared secret, and

where the second station produces said responsive message by veiling the hashed version of the next data random key using a second conversion array seeded by said shared secret and encrypting the veiled hashed version of the next data random key; and

decrypting and unveiling the hashed version of the next data random key at the first station.

18. The method of claim 17, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, and including

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions, and

placing a byte of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values.

19. The method of claim 17, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Z bit positions in an order, and including

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Z and identifying one of said Z bit positions, and

placing a bit of said random key in each of said X sections at the one of said Z bit positions identified by the corresponding one of said X values.

20. The method of claim 18, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X

values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

using a random number generator seeded by said shared secret to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

placing a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

mapping the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

21. The method of claim 17, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

using a random number generator to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

placing a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

mapping the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

22. The method of claim 17, including upon request for initiation of a communication session, presenting to the second station a user interface for initiation of an authentication session including a compiled version of the session random key and parameters for one or more conversion arrays, said user interface including a prompt for entry of the shared parameter, and at least said shared secret.

23. The method of claim 15, including upon request for initiation of a communication session, presenting to the second station a user interface for initiation of an authentication session including a compiled version of the session random key and parameters for one or more conversion arrays, said user interface including a prompt for entry of the shared parameter, and at least said shared secret.

24. The method of claim 14, including executing a further exchange including

sending a message from the first station to the second station carrying said encryption key encrypted using a first shared secret to the second station, where the second station returns a message carrying a hashed version of said encryption key encrypted using said first shared secret, and decrypting said encryption key at the first station;

sending a message from the first station to the second station carrying said encryption key encrypted using a second shared secret, where the second station decrypts said encryption key, and returns a message to the first station carrying a hashed version of the encryption key encrypted using said second shared secret.

25. The method of claim 14, including executing a further exchange including

sending a message from the first station to the second station carrying said encryption key encrypted using a first shared secret to the second station, where the second station returns a message carrying a hashed version of said encryption key encrypted using said first shared secret, and decrypting said encryption key at the first station;

sending a message from the first station to the second station carrying said encryption key encrypted using a second shared secret, where the second station decrypts said encryption key, and returns a message to the first station carrying a hashed version of the encryption key encrypted using said second shared secret; and

sending a message from the first station to the second station carrying an

authentication signal indicating success or failure of mutual authentication and establishment of the encryption key, said authentication signal being encrypted using one of said intermediate data random keys from a previous exchange.

26. A data processing apparatus, comprising:

a processor, a communication interface adapted for connection to a communication medium, and memory storing instructions for execution by the data processor, the instructions including

logic to receive a request via the communication interface for initiation of a communication session between a first station and a second station;

logic to provide ephemeral encryption keys at the first station; and

logic to execute after receiving said request, a plurality of exchanges of messages across said communication medium to mutually authenticate the first station and the second station and to provide one of said ephemeral encryption keys to the second station for use in said communication session.

27. The apparatus of claim 26, wherein during said plurality of exchanges, said instructions include logic requiring the first and second stations to use at least two shared secrets without exchanging messages carrying said shared secrets via the communication medium.

28. The apparatus of claim 26, said instructions include logic for mutual authentication based on at least two shared secrets without exchanging messages carrying said shared secrets via the communication medium.

29. The apparatus of claim 26, wherein said plurality of exchanges comprise interactive exchanges, said interactive exchanges including a message from the first station to the second station and a responsive message from the second station to the first station, where the responsive message comprises information from the message from the first station derived using information derived from a message in a previous exchange.

30. The apparatus of claim 26, wherein said logic to provide ephemeral encryption keys at the first station includes:

logic that assigns a session random key in said first station, in response to a request received during a session random key initiation interval for use in a first exchange of said plurality of exchanges;

logic that associates, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and

wherein said plurality of exchanges includes at least one message carrying an encrypted version of one of said plurality of intermediate data random keys to be accepted as said encryption key upon said mutual authentication.

31. The apparatus of claim 26, wherein said logic to provide ephemeral encryption keys at the first station includes instructions:

providing a buffer at the first station;

generating keys and storing said keys in the buffer;

associating respective session random key initiation intervals with said keys stored in said buffer;

using keys from said buffer as session random keys in response to requests received by said first station during said respective session random key initiation intervals for use in a first exchange of said plurality of exchanges;

removing keys from said buffer after expiry of the respective session random key lifetime in the buffer.

32. The apparatus of claim 31, wherein said buffer is managed as a circular buffer.

33. The apparatus of claim 31, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a multiple M times said value session random key lifetime to engage into establishing a communication session, where M is less than or equal to 10.

34. The apparatus of claim 31, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a multiple M times said value session random key lifetime to engage into establishing a communication session, and the session random key lifetime to engage into establishing a communication session is less than about 90 second.

35. The apparatus of claim 26, wherein said logic to provide ephemeral encryption keys at the first station includes instructions:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;

wherein said plurality of exchanges includes a first message from the first station carrying said session random key to the second station, where the second station returns a second message carrying a shared parameter encrypted using the session random key; and

decrypting the shared parameter from said second message at the first station.

36. The apparatus of claim 26, wherein said logic to provide ephemeral encryption keys at the first station includes instructions:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;

wherein said plurality of exchanges includes

a first exchange including sending a first message from the first station carrying

said session random key to the second station, where the second station returns a second message carrying a shared parameter encrypted using the session random key, and decrypting the shared parameter at the first station to validate the second station; and

a second exchange including sending a further message from the first station to the second station, the further message carrying a particular data random key from said plurality of intermediate data random keys encrypted using the session random key, where the second station returns another message carrying a hashed version of said particular data random key encrypted using said particular encryption key to the first station, and decrypting said hashed version of said particular data random key at the first station using said particular data random key.

37. The apparatus of claim 26, wherein said logic to provide ephemeral encryption keys at the first station includes instructions:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and

after said request for initiation of a communication session, presenting to the second station a user interface along with the session random key, said user interface including a prompt for entry of a shared parameter and at least one shared secret.

38. The apparatus of claim 26, wherein said logic to provide ephemeral encryption keys at the first station includes instructions:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and

after said request for initiation of a communication session, presenting to the second station a user interface along with the session random key, said user interface including a prompt for entry of a shared parameter and at least two shared secrets.

39. The apparatus of claim 26, wherein said logic to provide ephemeral encryption keys at the first station includes instructions:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;

wherein said plurality of exchanges includes

a first exchange including sending a first message from the first station carrying said session random key to the second station, where the second station returns a second message carrying a shared parameter encrypted using the session random key, and decrypting the shared parameter at the first station; and

a second exchange including sending a third message from the first station to the second station, the third message carrying a particular data random key from said plurality of intermediate data random keys encrypted using the session random key, where the second station returns a fourth message carrying a hashed version of said particular data random key encrypted using said particular data random key to the first station, and decrypting said hashed version of said particular data random key at the first station using said particular data random key;

and then executing at least one additional exchange in said plurality of exchanges, where

said at least one additional exchange includes sending an additional message from the first station to the second station carrying a next data random key from the plurality of intermediate data random keys associated with said request, encrypted using a key exchanged during a previously completed exchange in said plurality of exchanges, where the second station decrypts said next data random key and returns a responsive message carrying a hashed version of said next data random key encrypted using said next data random key, and decrypting at the first station said hashed version of said next data random key using said next data random key.

40. The apparatus of claim 39, including logic executing during at least one of said additional exchanges, including instructions

producing said third message by first veiling the particular data random key using a first conversion array seeded by a first shared secret and encrypting the veiled particular data random key, where the second station decrypts and unveils said particular data random key using the first shared secret, and where the second station produces said fourth message by veiling the hashed version of the particular data random key using a second conversion array seeded by said first shared secret and encrypting the veiled hashed version of the next data random key; and

decrypting and unveiling the hashed version of the particular data random key at the first station.

41. The apparatus of claim 39, including logic executing more than one of said additional exchanges.

42. The apparatus of claim 39, including logic executing during at least one of said additional exchanges, including instructions

producing said additional message by first veiling the next data random key using a first conversion array seeded by a shared secret and encrypting the veiled next data random key, where the second station decrypts and unveils said next data random key using the shared secret, and

where the second station produces said responsive message by veiling the hashed version of the next data random key using a second conversion array seeded by said shared secret and encrypting the veiled hashed version of the next data random key; and

decrypting and unveiling the hashed version of the next data random key at the first station.

43. The apparatus of claim 42, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, and including instructions

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions, and

placing a byte of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values.

44. The apparatus of claim 42, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Z bit positions in an order, and including instructions

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Z and identifying one of said Z bit positions, and

placing a bit of said random key in each of said X sections at the one of said Z bit positions identified by the corresponding one of said X values.

45. The apparatus of claim 42, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including instructions

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

using a random number generator seeded by said shared secret to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

placing a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

mapping the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

46. The apparatus of claim 42, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including instructions

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

using a random number generator to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

placing a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

mapping the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

47. The apparatus of claim 42, including upon request for initiation of a communication session, logic to present to the second station a user interface for

initiation of an authentication session including a compiled version of the session random key and parameters for one or more conversion arrays, said user interface including a prompt for entry of the shared parameter, and at least said shared secret.

48. The apparatus of claim 40, including upon request for initiation of a communication session, logic to present to the second station a user interface for initiation of an authentication session including a compiled version of the session random key and parameters for one or more conversion arrays, said user interface including a prompt for entry of the shared parameter, and at least said shared secret.

49. The apparatus of claim 39, including logic executing a further exchange including instructions

sending a message from the first station to the second station carrying said encryption key encrypted using a first shared secret to the second station, where the second station returns a message carrying a hashed version of said encryption key encrypted using said first shared secret, and decrypting said encryption key at the first station;

sending a message from the first station to the second station carrying said encryption key encrypted using a second shared secret, where the second station decrypts said encryption key, and returns a message to the first station carrying a hashed version of the encryption key encrypted using said second shared secret.

50. The apparatus of claim 39, including logic executing a further exchange including instructions

sending a message from the first station to the second station carrying said encryption key encrypted using a first shared secret to the second station, where the second station returns a message carrying a hashed version of said encryption key encrypted using said first shared secret, and decrypting said encryption key at the first station;

sending a message from the first station to the second station carrying said encryption key encrypted using a second shared secret, where the second station decrypts said encryption key, and returns a message to the first station carrying a hashed version of the encryption key encrypted using said second shared secret; and

sending a message from the first station to the second station carrying an authentication signal indicating success or failure of mutual authentication and establishment of the encryption key, said authentication signal being encrypted using one of said intermediate data random keys from a previous exchange.

51. An article, comprising:

machine readable data storage medium having computer program instructions stored therein for establishing a communication session on a communication medium between a first data processing station and a second data processing station having access to the communication medium, said instructions comprising:

logic to receive a request via the communication interface for initiation of a communication session between the first station and the second station;

logic to provide ephemeral encryption keys at the first station; and

logic to execute after receiving said request, a plurality of exchanges of messages across said communication medium to mutually authenticate the first station and the second station and to provide one of said ephemeral encryption keys to the second station for use in said communication session.

52. The article of claim 51, wherein during said plurality of exchanges, said instructions include logic requiring the first and second stations to use at least two shared secrets without exchanging messages carrying said shared secrets via the communication medium.

53. The article of claim 51, said instructions include logic for mutual authentication based on at least two shared secrets without exchanging messages carrying said shared

secrets via the communication medium.

54. The article of claim 51, wherein said plurality of exchanges comprise interactive exchanges, said interactive exchanges including a message from the first station to the second station and a responsive message from the second station to the first station, where the responsive message comprises information from the message from the first station derived using information derived from a message in a previous exchange.

55. The article of claim 51, wherein said logic to provide ephemeral encryption keys at the first station includes:

logic that assigns a session random key in said first station, in response to a request received during a session random key initiation interval for use in a first exchange of said plurality of exchanges;

logic that associates, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and

wherein said plurality of exchanges includes at least one message carrying an encrypted version of one of said plurality of intermediate data random keys to be accepted as said encryption key upon said mutual authentication.

56. The article of claim 51, wherein said logic to provide ephemeral encryption keys at the first station includes instructions:

providing a buffer at the first station;

generating keys and storing said keys in the buffer;

associating respective session random key initiation intervals with said keys stored in said buffer;

using keys from said buffer as session random keys in response to requests received by said first station during said respective session random key initiation intervals for use in a first exchange of said plurality of exchanges;

removing keys from said buffer after expiry of the respective session random key lifetimes in the buffer.

57. The article of claim 56, wherein said buffer is managed as a circular buffer.

58. The article of claim 56, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a multiple M times said value of session random key lifetime to engage into establishing a communication session, where M is less than or equal to 10.

59. The article of claim 56, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a multiple M times said value, and the session random key lifetime to engage into establishing a communication session is less than about 90 seconds.

60. The article of claim 51, wherein said logic to provide ephemeral encryption keys at the first station includes instructions:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;

wherein said plurality of exchanges includes a first message from the first station carrying said session random key to the second station, where the second station returns a second message carrying a shared parameter encrypted using the session random key; and

decrypting the shared parameter from said second message at the first station.

61. The article of claim 51, wherein said logic to provide ephemeral encryption keys at the first station includes instructions:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during

said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;

wherein said plurality of exchanges includes

a first exchange including sending a first message from the first station carrying said session random key to the second station, where the second station returns a second message carrying a shared parameter encrypted using the session random key, and decrypting the shared parameter at the first station to validate the second station; and

a second exchange including sending a further message from the first station to the second station, the further message carrying a particular data random key from said plurality of intermediate data random keys encrypted using the session random key, where the second station returns another message carrying a hashed version of said particular data random key encrypted using said particular encryption key to the first station, and decrypting said hashed version of said particular data random key at the first station using said particular data random key.

62. The article of claim 51, wherein said logic to provide ephemeral encryption keys at the first station includes instructions:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and

after said request for initiation of a communication session, presenting to the second station a user interface along with the session random key, said user interface including a prompt for entry of a shared parameter and at least one shared secret.

63. The article of claim 51, wherein said logic to provide ephemeral encryption keys at the first station includes instructions:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges; and

after said request for initiation of a communication session, presenting to the second station a user interface along with the session random key, said user interface including a prompt for entry of a shared parameter and at least two shared secrets.

64. The article of claim 51, wherein said logic to provide ephemeral encryption keys at the first station includes instructions:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges;

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges;

wherein said plurality of exchanges includes

a first exchange including sending a first message from the first station carrying said session random key to the second station, where the second station returns a second message carrying a shared parameter encrypted using the session random key, and decrypting the shared parameter at the first station; and

a second exchange including sending a third message from the first station to the second station, the third message carrying a particular data random key from said plurality of intermediate data random keys encrypted using the session random key, where the second station returns a fourth message carrying a hashed version of said particular data random key encrypted

using said particular data random key to the first station, and decrypting said hashed version of said particular data random key at the first station using said particular data random key;

and then executing at least one additional exchange in said plurality of exchanges, where

said at least one additional exchange includes sending an additional message from the first station to the second station carrying a next data random key from the plurality of intermediate data random keys associated with said request, encrypted using a key exchanged during a previously completed exchange in said plurality of exchanges, where the second station decrypts said next data random key and returns a responsive message carrying a hashed version of said next data random key encrypted using said next data random key, and decrypting at the first station said hashed version of said next data random key using said next data random key.

65. The article of claim 64, including logic executing during at least one of said additional exchanges, including instructions

producing said third message by first veiling the particular data random key using a first conversion array seeded by a first shared secret and encrypting the veiled particular data random key, where the second station decrypts and unveils said particular data random key using the first shared secret, and where the second station produces said fourth message by veiling the hashed version of the particular data random key using a second conversion array seeded by said first shared secret and encrypting the veiled hashed version of the next data random key; and

decrypting and unveiling the hashed version of the particular data random key at the first station.

66. The article of claim 64, including logic executing more than one of said additional exchanges.

67. The article of claim 67, logic executing during at least one of said additional exchanges, including instructions

producing said additional message by first veiling the next data random key using a first conversion array seeded by a shared secret and encrypting the veiled next data random key, where the second station decrypts and unveils said next data random key using the shared secret, and

where the second station produces said responsive message by veiling the hashed version of the next data random key using a second conversion array seeded by said shared secret and encrypting the veiled hashed version of the next data random key; and

decrypting and unveiling the hashed version of the next data random key at the first station.

68. The article of claim 67, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, and including instructions

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions, and

placing a byte of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values.

69. The article of claim 67, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Z bit positions in an order, and including instructions

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Z and identifying one of said Z bit positions, and

placing a bit of said random key in each of said X sections at the one of said Z bit positions identified by the corresponding one of said X values.

70. The article of claim 68, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including instructions

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

using a random number generator seeded by said shared secret to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

placing a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

mapping the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

71. The article of claim 67, where the one of the first and second conversion arrays comprises X sections, each of said X sections including Y byte positions in an order, each of said Y byte positions including B bit positions in an order, and including instructions

generating one of the first and second conversion arrays using a random number generator seeded by said shared secret to produce a first pseudorandom number having X values corresponding with respective sections of said X sections, the X values each being between 1 and Y and identifying one of said Y byte positions,

using a random number generator to produce a second pseudorandom number having B values corresponding with respective bits in a byte of said random key, the B values each being between 1 and B and identifying one of said B bit positions,

placing a byte, including B bits, of said random key in each of said X sections at the one of said Y byte positions identified by the corresponding one of said X values, and

mapping the B bits of said byte of said random key to said B bit positions identified by the corresponding one of said B values.

72. The article of claim 67, including upon request for initiation of a communication session, logic to present to the second station a user interface for initiation of an authentication session including a compiled version of the session random key and parameters for one or more conversion arrays, said user interface including a prompt for entry of the shared parameter, and at least said shared secret.

73. The article of claim 65, including upon request for initiation of a communication session, logic to present to the second station a user interface for initiation of an authentication session including a compiled version of the session random key and parameters for one or more conversion arrays, said user interface including a prompt for entry of the shared parameter, and at least said shared secret.

74. The article of claim 64, including logic executing a further exchange including instructions

sending a message from the first station to the second station carrying said encryption key encrypted using a first shared secret to the second station, where the second station returns a message carrying a hashed version of said encryption key encrypted using said first shared secret, and decrypting said encryption key at the first station;

sending a message from the first station to the second station carrying said encryption key encrypted using a second shared secret, where the second station decrypts said encryption key, and returns a message to the first station carrying a hashed version of the encryption key encrypted using said second shared secret.

75. The article of claim 64, including logic executing a further exchange including instructions

sending a message from the first station to the second station carrying said encryption key encrypted using a first shared secret to the second station, where the second station returns a message carrying a hashed version of

said encryption key encrypted using said first shared secret, and decrypting said encryption key at the first station;

sending a message from the first station to the second station carrying said encryption key encrypted using a second shared secret, where the second station decrypts said encryption key, and returns a message to the first station carrying a hashed version of the encryption key encrypted using said second shared secret; and

sending a message from the first station to the second station carrying an authentication signal indicating success or failure of mutual authentication and establishment of the encryption key, said authentication signal being encrypted using one of said intermediate data random keys from a previous exchange.